DUALITIES OF FINITE PROJECTIVE PLANES

BY

RICHARD WILLIAM BALL

A.B., University of Illinois, 1944

A.M., University of Illinois, 1945

AN ABSTRACT OF A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN MATHEMATICS
IN THE GRADUATE COLLEGE OF THE UNIVERSITY
OF ILLINOIS, 1948

URBANA, ILLINOIS

1948

DUALITIES OF FINITE PROJECTIVE PLANES

BY

RICHARD WILLIAM BALL

A.B., University of Illinois, 1944

A.M., University of Illinois, 1945

AN ABSTRACT OF A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN MATHEMATICS
IN THE GRADUATE COLLEGE OF THE UNIVERSITY
OF ILLINOIS, 1948

URBANA, ILLINOIS

1948

R. UNIV.
BIBLIOTHEEK
LEIDEN

DUALITIES OF FINITE PROJECTIVE PLANES*

Definitions. A duality is a one-to-one correspondence δ of a point P (line h) to a line P^δ (point h^δ) with the property that $P<h$ if, and only if, $h^\delta<P^\delta$. A point P (line h) is an absolute point (line) of the duality δ if $P<P^\delta$ ($h^\delta<h$). Let the number of absolute points of the duality δ be $N(\delta)$.

Theorem 1. $N(\delta) \neq 0$.

This is derived from number-theoretical considerations. For every finite plane there exists a unique integer $n\geq 2$ such that the plane contains n^2+n+1 points and every line contains exactly $n+1$ points. Let $C(m)$ be the number of ordered sets of points $P_1, P_2, \ldots, P_m$ such that $P_j<P_{j-1}^\delta$ for $j = 2,3,\ldots,m$ and $P_1<P_m^\delta$. It is proved for odd m that

$$(1)\quad C(m) = (n+1)^m + n^{\frac{1}{2}(m-1)}\left[N(\delta^m)-n-1\right],$$

and for odd primes p,

$$(2)\quad C(p^{i+1}) \equiv C(p^i) \bmod p^{i+1}.$$

Substituting (1) in (2) for $i = 0$,

$$(3)\quad (n+1)^p + n^{\frac{1}{2}(p-1)}\left[N(\delta^p)-n-1\right] \equiv N(\delta) \bmod p.$$

If p divides n, this reduces to

$$(4)\quad 1 \equiv N(\delta) \bmod p.$$

In a parallel manner we show that if 2 divides n,

*The author wishes to express his appreciation to Professor Reinhold Baer who directed the preparation of the thesis of which this is an abstract.

(5) $1 \equiv N(\delta) \bmod 2$.

But since $n \geq 2$ there is always at least one prime p which divides n, proving Theorem 1.

For applications, (1) and (2) yield for p an odd prime which is prime to n,

(6) $N(\delta^{p^{i+1}}) \equiv N(\delta^{p^i}) \bmod p^{i+1}$

if n is a quadratic residue mod p, and

(7) $N(\delta^{p^i}) + N(\delta^{p^{i+1}}) \equiv 2(n+1) \bmod p^{i+1}$

if n is a quadratic non-residue mod p.

These two congruences form the basis for the remaining theorems. Let $R(2o(\delta^2))$ be the group of those residue classes prime to $2o(\delta^2)$, the order of δ.

Theorem 2. If n is a square, $N(\delta^i) = N(\delta)$ for all i in $R(2o(\delta^2))$.

Proof. If i is in R, then $(i, 2o(\delta^2)) = 1$. By a Theorem of Dirichlet*, there are infinitely many primes p of the form $i + x2o(\delta^2)$ for variable x. For each $\delta^p = \delta^{i+x2o(\delta^2)} = \delta^i$, and n is a quadratic residue mod p. Applying (6) with i = 0, $N(\delta^i) = N(\delta^p) \equiv N(\delta) \bmod p$. This congruence holds for an infinity of moduli and is thus an equality.

If n is not a square, the method is essentially the same, but the results are more interesting. Professor Ivan Niven gave suggestions which lead to the following characterization of the group $R(2o(\delta^2))$ if n is not a square.

*E. Hecke, Vorlesungen über die Theorie der Algebraischen Zahlen, Akademische Verlagsgesellschaft, 1923, Theorem 131, page 170.

Theorem 3. Let $n = n^*n'$ where n^* is the largest square dividing n and where $n'>1$. The following statements imply each other.

(1) J is a subgroup of index 2 in R, where J is the set of all i in R such that there exist infinitely many primes p in the class i with n a quadratic residue mod p.

(2) There is no i in R such that the residue class of i contains primes p and q with n a quadratic residue mod p and non-residue mod q.

(3) If $n' \equiv 1 \bmod 4$, then n' divides $o(\delta^2)$.

If $n' \not\equiv 1 \bmod 4$, then $2n'$ divides $o(\delta^2)$.

This is proved by use of the theorem of Dirichlet and the quadratic residue theorems. On the basis of this and the congruences (6) and (7), we prove

Theorem 4. If n is not a square, then $n=n^*n'$ where n^* is the largest square dividing n. Then there exists a j in R such that $N(\delta^j) \neq n+1$ if, and only if, for i in J, $N(\delta^i) = N(\delta) \neq n+1$ and for i in R but not in J, $N(\delta^i) = 2(n+1)-N(\delta) \neq n+1$. These statements imply the following three equivalent statements.

(1) J is a subgroup of index 2 in R,

(2) If i is in J, n is a quadratic residue mod p for all primes p in i; if i is in R but not in J, n is a quadratic non-residue mod p for all primes p in i.

(3) If $n' \equiv 1 \bmod 4$, then n' divides $o(\delta^2)$.

If $n' \not\equiv 1 \bmod 4$, then $2n'$ divides $o(\delta^2)$.

VITA

Richard William Ball was born August 16, 1923, in Streator, Illinois. He attended public schools in Metropolis, Illinois, and Cairo, Illinois, where he was graduated from Cairo High School in 1941. He attended the University of Illinois where he received the degree of Bachelor of Arts in 1944 and the degree of Master of Arts in 1945. He was a scholar in mathematics 1944-1945 and fellow in mathematics in 1945-1946 and 1946-1947. He is a member of Phi Beta Kappa and Phi Kappa Phi.

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41549818_0251